

Digital Watermarks as a Gateway and Control Mechanism

Related Application:

Applicant claims priority of co-pending application 60/183,681 entitled "Digital Watermarks as a Gateway and Control Mechanism".

Field of the Invention:

The present invention relates to Internet communication and more particularly to using digital watermarks to as control elements in Internet communication.

Background of the Invention:

The Internet presents security challenges to corporations and others who have computers which store confidential information and which have connections to the internet.

Traditionally, documents containing confidential information are marked with a legend or other visual indicia with words such a "CONFIDENTIAL", "PROPRIETARY", etc. The presence of these marks alert anyone handling such documents that they should only be transferred outside of company under special precautions. It is relatively difficult and unusual for someone to inadvertently manually send such a document to an unauthorized receiver. However, the use of Internet communication changes the situation.

The Internet and electronic mail speeds the communications process; however, the Internet and electronic mail also make it much easier to inadvertently or accidentally send a confidential document to an unauthorized receiver. A single accidental or inadvertent keystroke can have wide raging unintended consequences. The Internet and other

1 electronic communication system make it easy to communicate; however, these systems
2 and networks also makes it easy to mistakenly or inadvertently sent a document to the
3 wrong party.

4
5 **Summary of the present invention:**

6 The present invention utilizes digital watermarks to control the transmission and/or receipt
7 of documents transmitted over computer networks such as the Internet. The invention
8 can be used to prevent the accidental dissemination of information to unauthorized
9 receivers. Furthermore, while no security system is fool-proof, the present invention helps
10 guards against the intentional, but unauthorized, dissemination of confidential information
11 to unauthorized receivers.

12
13 Most electronically transmitted messages contain text. However, electronic mail systems
14 generally allow images (i.e. pictures) or sound bites to be embedded into and form part of
15 a message. For example, a message can contain a "stamp" with the word "confidential"
16 or a message can contain a sound clip with the word "confidential". An image or sound
17 clip that forms part of an electronic message can carry a digital watermark that can be
18 detected and read by conventional watermark reading programs.

19
20 The "payload" or digital data in a digital watermark typically has a number of different
21 fields. One or more of these fields can be dedicated to a flags which indicates that the
22 document or image containing the watermark is confidential or otherwise classified and
23 that it should only be disseminated in a particular manor.

24

1 Typically, e-mail enters a transmission network by way of an e-mail server. Programs that
2 can detect and read watermarks are well known and commercially available. With the
3 present invention, the e-mail server passes each e-mail messages through a watermark
4 detection and reading program prior to sending the message out over a network. If the
5 watermark program detects a watermark, it interrogates certain flag bits to determine how
6 the message should be handled. For example, if the watermark reading program finds
7 that a particular flag is set, it can take action such as alerting both the sender and a
8 network administrator. If the watermark program finds no watermark or finds that a
9 particular flag is not set, the message is sent over the network in a conventional manner.
10 Alternately, the message can be sent only if a particular flag is set.

11
12 Thus, the present invention can serve as a control mechanism for controlling the
13 dissemination and receipt of electronic messages.

14
15 Messages and documents also enter the Internet and other electronic networks from
16 servers such as Web servers and FTP servers. In a similar fashion a watermark detection
17 program can interrogate documents on servers such as Web and FTP servers and take
18 action as described above.

19
20 **Brief Description of the Figures:**

21 Figure 1 is a diagram with an image containing the words "Confidential".

22 Figure 2 is diagram of the fields in a typical watermark.

23 Figure 3 is a diagram of a typical e-mail system.

24 Figure 4 is a more detailed diagram of the watermark reading and detection program
25 shown in Figure 3.

09784391-021501
FOUO

1

2 **Description of Preferred Embodiment:**

3 The embodiments of the invention described herein relate to systems for transmitting e-
4 mail messages over the Internet. This first embodiment has the ability to prevent the
5 accidental dissemination of confidential e-mail messages and documents to unauthorized
6 users. That is, the first embodiment of the invention prevents the transmission of
7 confidential e-mail or documents to anyone. An alternate embodiment merely prevent the
8 transmission of confidential documents to "unauthorized" users. That is, if a message is
9 sent to two recipients, one of whom is authorized and one of whom is not authorized, the
10 documents are transmitted to authorized user and not transmitted to unauthorized user. It
11 is very easy to add addressees to an e-mail message. Someone may address an e-mail
12 message which contains confidential information to a large group of people without
13 realizing the one of the addressee is not authorized to receive confidential information.
14 The system of the present invention will prevent such an e-mail from being transmitted to
15 the unauthorized person even though the sender included the address of that person in
16 the list of addressee. Another alternative embodiment can take a variety of actions such
17 as logging messages or sending them to an administrator in addition to preventing them
18 from being disseminated.

19

20 A typical confidential document 10 is represented in Figure 1. The document 10 can
21 either be an e-mail message, or alternatively it may be a document that is attached to an
22 e-mail message. The document 10 includes a confidentiality stamp 11 and lines of text.
23 The confidentiality stamp 11 is an image that has the word "confidential" superimposed
24 over a background that has a variety of lines. That is, the background in image 11
25 contains lines the width of which are varied to carry a watermark in accordance with the

AD
CONF

09784391.021501
FOI 20160426

1 teachings of US application 09/074,034, filed May 6, 1998 (which corresponds to PCT
2 application PCT/US99/08252), and US application 09/127,503, filed July 31, 1998 (which
3 corresponding to PCT application PCT/US99/14532). The disclosures of the above
4 referenced patent applications are hereby incorporated herein in their entireties by
5 reference. Alternatively the background of image 11 may comprise a weave or tint pattern
6 that carries a watermark. In still another alternative embodiment instead of having an
7 image 11 embedded in the message, the message may contain an audio clip with the
8 work confidential. The audio clip would be watermarked using conventional audio
9 watermarking techniques. However, in the first embodiment described herein the, image
10 11 has both a human readable word "Confidential" and a digital watermark that can be
11 read by a watermark detection and reading program.

12
13 The data fields and flags in a typical watermark payload are shown in Figure 2. It should
14 be understood that the fields and flags shown are merely representative and they can take
15 may alternative forms. The first embodiment of the invention utilizes one of the flag fields
16 to indicate that a particular document is confidential. The other fields can be used in a
17 conventional manner. Alternate embodiments can use a number of flags to indicate
18 actions that should be taken with a particular message.

19
20 Figure 3 shows a typical e-mail system. A relatively large number of individual user
21 terminal 301 are connected to an e-mail server 302. Only five representative terminals
22 designated 301a to 301x are shown for convenience of illustration. The terminals 301 are
23 connected to server 302 by conventional connections such as by an Ethernet LAN or by
24 dial up modems. The e-mail server 302 has a conventional interface 303 to the Internet
25 and it receives and sends messages from the individual users to the Internet. The e-mail

1 server 302 is conventional and the details of the e-mail server 302 forms no part of the
2 present invention. However, with the present invention, before the e-mail server 302
3 transmits a message from one of the individual user terminals 301a to 301x to the
4 Internet, the e-mail server passes the message through a watermark detection and
5 reading program 305. Both the e-mail message itself and any attached documents are
6 passed through the watermark reading program. The watermark detection and reading
7 program 305 determines if a message contains a watermark. If a watermark is detected,
8 the confidentiality flag bit is interrogated. If the watermark reading program 305
9 determines that the flag bit is set to "confidential", the first embodiment of the invention
10 merely informs the e-mail server 302 to return the message to the sender. Thus, the first
11 embodiment of the invention prohibits any confidential information from being transmitted
12 as part of an e-mail message.

13
14 A second embodiment of the invention provides for a wider array of alternative. As shown
15 in Figure 4, the second embodiment of the invention includes a data base 401. The data
16 base 401 contains a list of different potential message senders, a list showing different
17 groups of potential message recipients, and a set of possible categories indicated by the
18 setting of the various flags in a message. For example, the senders may fall into three
19 groups designated sender groups S1, S2 and S3. The potential recipients can fall into
20 three groups designated R1, R2, and R3. The data base 401 and the associated logic
21 402 can implement logic rules such as indicated by the following table:

Sender Group	Recipient Group	Flag Conditions	Action
S1	R1	011	Send message
S1	R2	110	Do not sent message notify the administrator

S1	R2	001	Send message, and log fact that S1 sent a message to R2.
S1	R2	101	Return message to sender
S2	R1	011	Send message
S2	R3	110	Do not sent message and notify the system administrator

1

2 It should be clearly noted that the above is merely a simplified example of the rules and
3 combinations that could be in data base 401. The data bases could include hundreds or
4 thousands of users and it could include dozens of rules. The system can be complex or
5 simple as desired for a particular application. A system can include many alternatives in
6 addition to those shown above or a system might include only a very few alternatives. For
7 example, the system could include only a list of addresses which are authorized to receive
8 messages which have a confidentiality flag set to "confidential". Such a system would
9 allow confidential documents to be only sent to selected addresses. Alternatively or in
10 addition the system could include a list of individuals authorized to send confidential
11 documents. The system could merely check the sender against this list or alternatively,
12 the system could require that a password be entered when such messages are
13 encountered. The table above shows only three flag bits. A system could have more or
14 less flag bits as the needs of the particular system require.

15

16 The import point is that the system considers the message sender, the message recipient
17 and the condition of the flags in the data carried by a digital watermark to determine what
18 action should be taken. The digital watermark can be carried by the message using any
19 of the known ways of watermarking a document. For example, it can be carried by
20 modulating the width of lines or by modulating the luminosity of pixels in an image or by a
21 watermark in audio data.

1
 2
 3
 4
 5
 6
 7
 8
 9
 10
 11
 12
 13
 14
 15
 16
 17
 18
 19
 20
 21
 22

In alternate embodiments of the invention, the confidentiality stamp could include a watermark in an image by means other than using line width modulation as described with respect to the first embodiment of the invention. The background of the stamp could include a conventional image carrying a conventional watermark.

In an alternative embodiment of the invention, rather than checking for a digital watermark, the system could check for a text string such as "confidential" and take action in response to locating such a text string.

The above described embodiments relate to controlling the dissemination of information; however, it should be understood that the invention could be applied in similar manner to control the receipt of confidential information or to control the action taken when messages containing watermarks are received.

While the previously described embodiments apply to e-mail systems, similar precautions could be taken with FTP servers or with Web servers.

While the invention has been shown and described with respect to various preferred embodiments, it should be understood that various changes in form and detail could be made without departing from the scope and spirit of the invention.